European Journal of Academic Essays 4(3): 57-65, 2017
ISSN (online): 2183-1904
ISSN (print): 2183-3818
www.euroessays.org

Problematic Issues of Developing International Standards to Ensure Information Security

< Nugmanov Nugman >[1]

[1] The University of World Economy and Diplomacy,
54 Mustakillik Avenue, Tashkent, Uzbekistan
nugmann@mail.ru

Abstract: The article considers the ways of developing international standards and new mechanisms in the framework of the UN in realization of the unique approach to provide information security and progressive use of ICT.
Based on the analysis of the reports of the UN group of governmental experts to promote the consideration of existing and potential threats in the sphere of information security at multilateral levels, as well as, international legal norms in digital environment, various topical issues concerning the application of international law in the field of information and ensuring international information security are discussed. The author outlined the problems of digital environment on the following issues:

- A common interpretation of the wrongful use of ICT in the international law system;
- Developing relevant international legal framework for combating the use of ICTs in terrorist and criminal purposes;
- International legal support of human rights for the freedom to seek, receive and impart information;
- Protection of critically important information infrastructures; the role of information in the global network Internet.

There is no single common understanding of the international community regarding the identified problems and it will cause difficulty in preventing international conflicts involving ICTs. The main problematic task is to develop the criteria to apply international legal norms and methodologies of the adaptation of international law to international relations in the information environment
Keywords: principles of international law, international spread of information, international information security, ICT, information war, international information space.

---

1. Introduction

The emergence of the problem of information security issues is associated with one of the characteristics of the current stage of world scientific and technological progress along with the global information revolution. Because of this, extremely fast and almost universal availability of the newest information technologies and global communications occur and a kind of global information space is formed in the international society. However, the advances in information revolution can be used not only for positive purposes, but also for the purposes of ensuring the superiority of certain countries in the international arena over other countries with interfering their internal affairs. As a result, we can speak about the emergence of a fundamentally new area of international confrontation, affecting both the interests of the security of individual States and the overall system of international security at the global and regional levels. That is the reason why the problem of information security is relevant now.

Traditionally, security is understood as such a condition in which the vital interests of a person, a society, a nation and the international system are protected from any internal or external threat. According to Meshkova, international security can be defined as "the state of the society, which provides a reliable and comprehensive protection of individuals, society and the State in the information area from exposure of certain threats causing spontaneous or organized form of information and communication flow" [1]. However, there is a narrow, technical understanding of information security. For example, according to Professor Bashly, "information security is a protection of information and supporting its infrastructure from accidental or intentional effects of a natural or artificial character, which may cause damage to the owners or users of information" [2]. This definition given by professor Bashly is reinforced in another saying: "For its significance in the development of the society, information equates to the most important resources along with raw materials and energy"[3].

Thus, today the problem of information security does not belong to narrow technology categories, and moves into the realm of conceptual basis of management of public processes. This is why consideration of the problem of information security from the international legal point of view is particularly important. Mitrokhin believes that "Deep and comprehensive analysis of the impact of information, information security in modern conditions is becoming an essential requirement of the society. It is necessary to establish mechanisms to control a variety of factors such as establishment of information weapons and conducting information wars, expansion of information flows, bearing in

itself the possibility of increasing the scale of negative effects on the social systems of different levels, the advent of real possibility and ways of manipulative effects on mass and individual consciousness.

It is obvious that at this stage of human development, information and communication technologies (ICTs) have an enormous influence on the development of not only human beings, a society, a State, but also on the entire international community. Undoubtedly, the current development in the field of usage of ICT contributes to not only economic but also social and cultural development. Moreover, the positive achievements, except enumerated purposes, can be equally used in order to ensure the dominance of some States over others, for instance, by interfering in internal affairs of other countries. Certainly, it is considered as a breach of the Charter of the UNO. It is clear that the damage of the use of ICT for the purposes contrary to the principles of international law, as well as other destructive purposes, including terrorist, can be compared to the greatest destructive weapons. It should be noted that the impact of information weapons, scale and destructive degree, which is constantly increasing, can affect not only the Internet information resources, but also a variety of strategically important State objects. By using information weapons, economic disruption can be reached or at the same time, entire governmental structure can be ruined.

2.Review of the problems of the sphere of information security in the framework of the UNO.

Interstate relations in the field of information security, undoubtedly, are under the control of the norms and principles of international law, governing the various information security issues of the State. It should be noted that, in accordance with the UN General Assembly resolution adopted in Session 55, on July 10, 2000, international information security was defined as "the state of international relations, excluding breach of world stability and endangering the security of the states and world community in cyberspace» [4].

The topicality of information security at the international level is beyond the question and, evidently, for the progressive use of ICT it is required new mechanisms to be elaborated through the collective efforts of the entire international community. Therefore, the discussion of the various ways of ensuring international information security (IIS) mostly took place in the framework of the United Nations, which, for nearly two decades, has reflected the points about the role of the science and technology in the context of international security on its agenda.

Based on necessity of targeted and substantive discussion of issues of IIS at the level of the UN, on September 23, 1998 the draft of the resolution of the UN General Assembly entitled "Developments in the field of information and telecommunications in the context of international security" [5] was sent to the UN Secretary-General to consider. The draft, in particular, contained an invitation to all the United Nations Member States to inform their point of view to the Secretary-General on the use of information technology for military purposes, instantiation, hostile and unauthorized influence on information and communication systems and information resources. The draft of the resolution was revised in the first Committee on disarmament and international security, and on December 4, 1998 it was adopted by consensus of the UN General Assembly [6]. In 1999, the UN General Assembly adopted Resolution No. 54/49, in which the problem of illegal use of information and communication technologies was formulated for the first time.

The resolution of UN General Assembly of December 23, 1999 on developments in the field of informatization and telecommunications in the context of international security, expressed the concern that the proliferation and use of modern information technologies and media can potentially be used for the purposes inconsistent with the objectives of maintaining international stability and security [7]. The reason for this concern is the emergence of opportunities of the countries' hostile use of information and communication technologies in the various political and military purposes, including terrorist and criminal activities in the international information area.

On October 3, 2001, the UN Secretary General released report on the main threats in the information space. They are the followings: the development and use of unauthorized interference in the information environment of another State; misuse of foreign information resources and cause damage to them; deliberate information influence on the population of a foreign State; attempts to dominate in the information space; promotion of terrorism; maintenance of information wars[8].

Taking General Assembly resolution 53/70 dated December 4, 1998, 54/49, dated December 1, 1999 and 55/28 of November 20, 2000, and the results of the Ministerial Conference on terrorism, held in Paris on July 30, 1996, in the 56 session of the UN General Assembly on November 29, 2001, the Member States were encouraged to continue contributing to the study of the problem of international information security at the international level. Besides, possible measures to diminish the threats appearing in this sphere were also found important because of the necessity to keep the free flow of information. Furthermore, based on that resolution, in accordance with paragraph 4, in 2004 a group of governmental experts (GGE) was created to promote the consideration of existing and potential threats in the sphere of information security at multilateral levels [9]. The very group of governmental experts has become a major interstate tool to analyze the issues concerning international information security.

In 2007, on Session 62 of the UN General Assembly the draft resolution entitled "Developments in the field of information and telecommunications in the context of international security" aimed at preventing the use of information resources or technologies for criminal or terrorist purposes was considered [10]. The document calls for facilitating the consideration of existing and potential threats and measures, and resolving them in the field of information security at the international level, taking the significance of free flow of information into account. Based on this document, in 2009 the General Assembly of the UN created a new group of governmental experts to analyze the issues of international information security.

In 2011 the General Assembly unanimously adopted Resolution 66/24 [11], which called for further action based on the results of the last GGE. The new GGE was requested to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to neutralize them, taking into consideration the assessment and recommendations contained in the Report for

the year 2010; it was requested to submit a report on the 68th Session of the General Assembly in September 2013.

Based on the reports of the GGE for 2012, 2013 the UN General Assembly unanimously adopted Resolution 68/243 [12], in which it took note of the results of the work of the GGE for 2012, 2013 and General Secretary was instructed to establish a new GGE.

In the framework of the new GGE of the UN on IIS, which was created in 2014, the document embodying the universal interest of States in the peaceful use of ICT was formed. In this report, consensus was reached on the relative applicability of international law to the use of ICT, ended with the adoption of the UN Resolution A69/28 from December 2, 2014 [13].

In the framework of future meetings of the GGE, took place in 2015, the group found a compromise approach to solving legal problems arising in the global information space. The GGE on developments in the field of information and telecommunications were proposed recommendations in the context of international security. They disclosed various ways to promote an open, secure, stable, peaceful and affordable ICT environment [14].The level of discussion at the next convening of the group of governmental experts showed that the establishment of a comprehensive system of international information security is increasingly understood as a topical and a priority for action in the international community.

Based on the results of the work of the GGE 2014-2015, on the 70-Anniversary Session of the UN General Assembly Resolution 70/237 under the title "Developments in the field of information and telecommunications in the context of international security" was adopted by First Committee on December 23, 2015 [15]. Co-authors of the paper are more than 80 States, including BRICs, SCO, CIS, countries of Latin America and Asia. Among them the countries such as the United States, Japan and many EU member states, including Great Britain, Germany were represented as co-sponsors for the first time.

This document is based on a huge positive experience of the UN's GGE on international information security. The group convening of 2014-2015 timeframe was able to achieve consensus on a number of fundamental issues concerning the use of ICT, including the exclusively peaceful use of ICT, based on generally accepted international principles of non-use of force or threat of force, respect for sovereignty and non-interference in the internal affairs of States.

In addition, an important outcome of the GGE, the 4-th convocation was paragraph 12 concerning the Group's adoption of the rules of conduct in the field of ensuring international information security proposed by Kazakhstan, China, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan, submitted to the UN General Assembly in January 2015. One of the main purposes of these rules of conduct is to define the rights and duties of States in the information space, stimulating their constructive and responsible behavior. Furthermore, they include other aims like strengthening cooperation of the countries to confront common challenges and threats in the information space in order to create a peaceful, secure, open and collaborative information environment. Another goal was to use information and communication technologies, and information and communication networks to promote full social and economic development and the well-being of peoples, and to be compatible with the objectives of ensuring international peace and security [16].

A significant outcome of the GGE's fourth convocation is initiating a convocation of the group. It is known that the new fifth group of the governmental experts, which will include in its membership up to 25 countries, begins in August 2016. The new GGE aims to realize a peaceful use of ICT for national development and international stability, as well as the development of a common understanding of existing and potential threats in the sphere of information security and possible cooperative measures to eliminate them.

Based on the foregoing, it can be said that the UN keep a permanent, consistent and active discussion of problems of international information security , where States are currently trying to find a unified remedy against emerging threats in the digital environment .

3. Applied problems in the sphere of information security.

It should be noted that in the definition of "information security" it is necessary to take into account the elements of the notion of both "security" and "information". Meanwhile, as it has been already mentioned, the word "information" in the notion of "information security" refers not only to the concept of "information", but also to the area where the security is granted, namely in the information sphere.

It is obvious that without the widespread use of information technologies it is impossible to ensure economic growth and development, as well as a quick and qualitative execution of State functions. As noted in the report of the UNESCO "Information and communication technologies in the concept of development: UNESCO'S perspective," information and communication technologies have the ability to dramatically transform, give a new kind of ways in which people use to organize their own lives, communicate, participate in various spheres of public life. These technologies form the basis for a radical shift from industrial and post-industrial development definitions to move into a new phase based on the models of information societies [17].When defining information security, it is important to understand that it is a social rather than purely technological phenomenon. In this regard, the views of a number of scientists on information security like on the combination , first of all, of technical measures to protect information, including so-called firewalls, access control systems, antivirus software and other software and technical means and methods should be admitted not entirely reliable.

Surely, that information security involves the use of special technical means and methods to protect the information from unauthorized access, theft, destruction, etc. Nevertheless, there should not be the identification of these concepts. Otherwise, unduly it narrows the notion of information security, and the problem of information security is solely applied to technical means and methods. Consequently, information security is not only the protection of information, but also organizational, legal and other measures aimed at ensuring the sustainable development of the society and the State.

Because of advances in the field of information technologies, so-called informational space emerged in the international society. Many researchers name it cyberspace or information environment, defining it as significantly different

from the traditional environments - land, sea, air, outer space, in which humanity has already been implementing its expansion. The notion of "information security" is inseparably connected with the informational space, because mostly in this space the activities that may affect information security are performed.

The notion of "information security" is a very complex phenomenon. It is hence that there are different approaches to the formulation of the notion of "information security".

For example, the UN Secretary-General's report on the 55th session of the General Assembly on July 10, 2010 states that information security - the state of protection of the basic interests of the individual, the society and the State in the information area, including the information and telecommunications infrastructure and information on its properties such as integrity, objectivity, confidentiality and availability. The specified definition reflects two aspects of ensuring the two aspects of information security, but nonetheless, these aspects are not allocated clearly that can lead to difficulties in the application of the definition.

There are different approaches to the concept of "information security", for example, “The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability" [18]. In addition, «Information security is the protection of information and minimizes the risk of exposing information to unauthorized parties"[19]. Alternatively, "A well-informed sense of assurance that information risks and controls are in balance"[20].

The definition of "information security", proposed by Professor Lopatin, stated that information security should be understood as the state of protection of the national interests of the country (the vital interests of the individual, society and the State on a balanced basis) from internal and external threats in the field of information [21].

Some authors define the concept of "information security" in the broad and narrow sense: information security in a broad sense represents the state of protection of information resources, information channels and open access to any source of information of each citizen, public organization, a separate State as a whole. Information security in a narrow sense is a component of military security, relating to the protection of information resources, channels, data and knowledge bases, their processing and storage used purely for military purposes, which protect the vital interests of citizens, society and the State.

It should be noted that the measures aimed at ensuring protection of the interests of the individual, society and the State, including sustainable development, can be divided into measures relating to the information content, and measures relating to information and communication tools, which include the information they contain.

The first type of action includes a protection against information that is harmful or illegal, which has a negative impact on the consciousness of personality and so on. The second type of action includes legal and organizational measures aimed at maintaining the functioning of the information infrastructure, as well as ensuring its protection from any negative impacts.

Based on the above-mentioned ideas, it is possible to offer the following definition of "information security". Information security is the state of protection of the individual, society, the State from the information that is harmful or illegal, having a negative impact on the consciousness of personality that inhibit sustainable development of individuals, the society and the State.

Information security also provides sustainable development of the state of protection of the information infrastructure, including computers and information as well as telecommunication infrastructures and information they include.

We believe that the main threat for information security of the State is not a penetration into the information network in the territory of that State, but the negative impact on critically important structures. While the penetration of the specified structure from another State, even if the penetration has not resulted in substantive consequences, it constitutes a violation of the principle of the peaceful use of the information space. Penetration into other information structures other than critical is a violation of the principle of peaceful use, in case they have caused significant social, economic and other harmful effects.

4. Issues of implementation of international legal norms in the international information area.

Based on the analysis of the reports of the GGE and international legal norms in digital environment, we addressed some of the current issues concerning the application of the international law in the field of information and ensuring international information security.

It is important to mention that not all legal provisions that are applicable in various areas of human activity can be applied directly to the field of ICT. Today, criteria for the application of international legal standards and methodology adaptation of international law to international relations in the field of information have not been formed. It is clear that there is no single common understanding of the international community regarding the identified problems and it will contribute to the difficulty of preventing international conflicts involving ICTs.

One of the most important issues is the interpretation of the wrongful use of ICT within the system of international law. It is well known that, in international law there is no unified approach to such a notion as "war", so there is no longer a generally accepted definition of "information warfare". According to the doctrinal definition, information warfare is a use of information weapons to affect knowledge and imagination systems of the enemy [22]. There is also the view that information warfare is an attack of information-to-information.

In addition, it is pointed out that the information war is "a qualitatively new type of war, where information serves as a weapon and the fight is targeted to change public consciousness" [24].

Elaboration of a universally accepted definition about the concept of information warfare, despite the fact that such wording is included in certain international legal Acts, is complicated due to a number of specific properties inherent in the misuse of ICTs in resolving conflicts between States with power. Such peculiar properties include cross-border, namely the possibility to implement aggressive violent actions with ICTs without violating territorial boundaries.

It is known that the generally accepted principles of international law concerning such definitions as "Act of aggression", "use of force" or "armed attack" presuppose the

existence or use of weapons. At the same time, it should be mentioned that ICTs are not weapons themselves. This creates difficulty in applying the term "weapon" to ICTs and at present international laws defining attacks using ICT as an armed attack do not exist.

It should be noted that such a concept as "information weapon" is used in a number of international agreements adopted in the framework of the Shanghai Cooperation Organization and CIS. In an annex to the agreement on cooperation among CIS Member States in the field of information security from November 20, 2013 stated that "information weapons are information technologies, tools, and techniques used to conduct information warfare" [25].

The definition of "information warfare" is included in the agreement between the Governments of the Member States of the Shanghai Cooperation Organization on cooperation in the field of ensuring international information security adopted on June 16, 2009

In accordance with Article 1 of this agreement, "information warfare" is the struggle between two or more States in the information space with the intent of causing harm to information systems, processes and resources, and other critically important and other structures, undermining political, economic and social systems, the massive psychological manipulation of a population in order to destabilize society and the State, as well as compelling a State to take actions in the interests of the opposing side, and "information weapon is information technologies, tools, and techniques used to conduct information warfare" [26].

We believe that the existing approaches to the formulation of basic notions regarding the misuse of ICT for representing a threat to international peace, security and stability, can be used as a basis for the subsequent formation of generally accepted notion "information weapon".

It should also be noted the lack of a relevant international legal framework for combating the use of ICT for terrorist and criminal purposes.

Today, the existing mechanisms of international cooperation in the fight against terrorist and criminal uses of ICTs are not conducive to full and prompt receipt of evidence in the form of computer data. As traditional ways of international cooperation involve sending written queries that typically take a long time, and in the information space probative information by virtue of specificity can be quickly lost.

The main attempt to implement an effective multilateral mechanism in this area is Council of Europe Convention on Cybercrime of 2001 (Budapest Convention). However, the introduction of innovative ICT, as well as the rapid development of information space served as a mismatch of the Budapest Convention with modern realities. New different types of crime in the information sphere occurred, for example, the use of programs that can cause great damage, performing illegal actions, namely the so-called botnets. In addition, we can note that the Budapest Convention spared crimes such as "fishing" is a form of Internet fraud, etc. It is clear that to realize the combats against reemerging criminal acts in cyberspace without legal registration is very difficult.

In our opinion, one of the main unacceptable provisions of the Budapest Convention is vaguely worded provisions in accordance with which there is a possibility of Trans-border access to data in an investigation without the consent of the other party (art. 32). We believe that cross-border access to data when carrying out investigations violates the principle of State sovereignty.

We believe that, based on the positive practices of the Budapest Convention and recommendations of the GGE, it is necessary to develop an agreement at the level of the UN. It will fight against criminal activities in the international information area taking into account the current level of ICT development and information environment, no doubt based on the principle of respect for State sovereignty and non-interference in the internal affairs of another State.

Regarding the problem of ensuring human rights for freedom to seek, receive and impart information, it should be noted that one of the urgent tasks in the international information area is providing a balance between the freedom to seek, receive, disseminate all kinds of information, ideas and special responsibilities related with those rights, which contain limitations urging to respect the rights or reputations of others, and, consequently, it is related to the security of the State in the information area. We note that human rights and freedom "to seek, receive and impart information and ideas with the help of any media and regardless of frontiers" enshrined in the Universal Declaration of human rights in 1948 (Article 19) cannot be absolute. In Article 29 of the Declaration, it is recognized that in the execution of the rights and freedom of a person may be subject to restrictions. But, the following criteria should be followed: firstly, restrictions must be prescribed by law; secondly, restrictions may be imposed solely for the purpose of securing due recognition and respect for the rights and freedom of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society. For this, it is necessary to add the law of legislative restriction of freedom of information “to protect the State security”, “ the health and welfare of the population” included in the international Pact on citizen and political rights of 1966(Article 19).[27]

Based on the obligation to respect human rights to freedom of thought, freedom of expression, the State referring to the need to ensure security should be entitled not only to filter the Internet content but also to block the Internet sites that contain malicious content. The reason for this view is that deliberate malicious content developed under the guise of freedom of expression, as well as taking into account the infinite possibilities of the Internet tools related to circulation and commentary, it turned into acting information weapons to fulfill criminal and political objectives, like propaganda of ideas of terrorism, involvement of new sponsors in terrorist organizations, interventions in the internal affairs of sovereign countries, etc.

Additionally, when looking for the right balance between safeguarding human rights and security of the use of ICTs, there arise problems associated with the anonymity of the Internet, which makes it difficult to identify the identity and citizenship legally. These problems occur because of significant differences of national legislation about the placement of harmful information on the Internet.

In light of ensuring international information security, the problem of protecting so-called critical information infrastructures that save critically important objects or processes from harm should be taken into consideration. As it is well known, because of destructive information influence

on such infrastructure (national telecommunication systems, airports, natural gas pipelines, etc.) the catastrophic situation may arise and namely violations of such information systems can lead to a huge negative effects of national scale.

In order to ensure international security, it is suggested that international peremptory norm should consolidate the commitment of States on curbing attacks on critical information infrastructures of another State. To implement an international agreement requires the identification of such infrastructures for further international exchange of information on the subject. Thus, it is necessary to take into account that, because of such an international identification, critical information infrastructures may turn into a lightweight object for information attacks. We believe that the effectiveness of the State to ensure the security of critically important infrastructure can be achieved by the application of international experience implementing Resolution 58/199 of the UN General Assembly on the creation of a global culture of cyber security and the protection of the most important information infrastructures [28].

5. The regulation of international relations in the sphere of information security.

It is clear that information and communication technologies develop more than dynamically, at the same time the development of international legal norms in the field of ensuring international information security has been slow and may not adequately reflect existing digital reality. However, this is no reason to stop regulating inter-State relations, which are under the influence of norms and principles of international law. In view of the emergence and development of new modern ICT, it is necessary to form a system of measures for the application of the universally recognized norms and principles of international law to the peculiarities of global informatization.

In the light of the foregoing, we believe that the international community is faced with the task of elaborating an International Convention comprehensively regulating the whole range of problems concerning the misuse of ICT. It is necessary to note that this document should take into account the existence of threats to the IIS as a politico-military and criminal, including the threat of a terrorist nature as well. In this agreement, it is vital to examine the admissibility of collective measures to reduce damage to the national interests of individual States, and undoubtedly in the interest of the global community as a whole.

Also we consider that in order to form an effective system of IIS, which is capable to warn effectively about the threats to the peace due to hostile use of ICT, it is required to pay attention to further development of the international legal framework in line with the implementation of an effective system for the prevention and cessation of possible aggressive use of ICT.

In addition, when creating and using open international information networks and in organizing the exchange of information at the international level, it is necessary to develop interstate cooperation on the formation of international standards to implement a holistic approach to information security as an information resources and information and communication systems.

It should be notified that one of the main foundations of the information society is trust and security. Therefore, as the most important areas of action on confidence building and security in the use of ICTs, it is necessary to point out the following tasks:

- To promote cooperation between States in the framework of the United Nations and with all interested parties in the relevant forums to analyze existing and potential threats in the field of ICT, as well as other issues of information security and network security;
- To prevent and detect manifestations of cybercrime and misuse of ICTs with the help of the organs of State administration in cooperation with the private sector and to respond to these phenomena by developing appropriate guidelines;
- To study the legislation, which gives the ability to investigate effectively and prosecute the misuse of ICTs;
- To promote effective cooperation in this area, as well as prevention of computer incidents;
- To exchange the best practices in the field of information security and network security, and to promote their use by all relevant stakeholders;
- To appoint coordinators in all concerned countries to respond in real time to security incidents and an open interoperable network of coordinators to exchange information and technologies on response to the incident;
- To encourage the active participation of the interested countries in the UN activities to build confidence and security in the use of ICTs.

It should be noted that information is a powerful tool for shaping public opinion. Thus, information has a big impact on foreign and domestic policy of the State. Obviously, deepening the countries' mutual awareness of each other's lives, increasing international exchange of information on cultural, economic, social problems have contributed to a better understanding between nations and States. Delivering objective information to the public about international issues and possible solutions is a major factor in the maintenance of international peace and the strengthening of the international legal order. The increasing role of information and communication in the development of contemporary international relations, the special responsibility of States, as well as mass media for the distributed information require international legal settlement of problems related to international exchange of information. The important role of legal regulation of international information exchanges is confirmed in the attention given by the UN, UNESCO and other international organizations to develop international legal norms in this field. The penetration of information in all spheres of life, the importance of international exchange of information for all States, without exception, are putting the issue of information media management on a par with other global problems. The legal regulation of the issues of information and communication, therefore, should be broad and global in nature. The diversity of the mass media, the development of information technologies, the complexity of regulating relations in the information sphere, all of them lead to the formation of a new area that is information law. The proclamation of the freedom of the mass media, the abolition of censorship and the development of new technologies have led to a significant increase in the volume of information. On the background of lack of legal system of information flow, which is virtually uncontrollable, creates favorable environment for human rights violations.

Although there are a large number of national laws and many international laws in the area of human rights, yet many issues require further elaboration. Such issues include information freedom of the individual, in other words informational human rights. The legal status of a person is a system of rights, freedoms and obligations, defining the legal status of a person in a particular area of life, including in the field of information. In this regard, it is necessary to develop new legal norms ensuring the realization of the right to freedom of speech and pluralism of ideas, and to create effective mechanisms for their implementation.

Another important issue is unjustified disproportion between the two parties - the freedom of information and content information. Condemning the intentional interference as a denial of the right of everyone to be fully aware of all the news, views and ideas regardless of frontiers, the first documents in the mass media have underestimated the possibility of transmission of harmful information. Governments were asked to refrain from the transfer of information, which would become unfair attacks or slander against other nations, and strictly complies with the requirements of the ethics in the interest of international peace, sending messages about the facts truthfully and objectively. Moreover, today the possibility of using information technology by criminals should be seen as a potential danger. Cyber terrorism should be seen as an issue of interest to all States. The representatives of many countries have expressed the view that it is extremely important to promote appropriate measures to ensure the security of resources, i.e., the information infrastructure (to be understood by technical means and systems of formation, processing, storage and transmission of information) unilaterally and multilaterally as well. Cyber-terrorism is now the subject of analysis and design. Thus, the Council of Europe's Committee of Ministers adopted an amendment to the International Convention on Cybercrime dated November 13, 2002. In the United States, the concept of security in cyberspace is actively discussed. The fight against crimes in the field of information and telecommunications technologies has become a priority in the activities of the intelligence services, along with the fight against terrorism and counterintelligence. The new items of reference, such as information security, cyber terrorism, e-commerce have to develop, and so do the new forms of control. Therefore, cooperation of all States in the area of international exchange of information is pivotal.

In connection with that, the individual States and the international community as a whole have taken concrete steps to ensure the integrity of their information space. The resolutions of the specialized agencies of the UN are not binding; however, they can play a big role in the development of the standards of law, the definition of concepts and concretization of the policies of organizations.

Therefore, we can say that the combination of General Conference resolutions on information affairs symbolizes the emergence of a new Institute of law. Among the most significant documents that define the trends of the international exchange of information, adopted recently include the declaration on “Right to know. Access to information in European countries” adopted by the Conference of the European Federation of journalists (EFJ) (April 27, 1996), the Sofia Declaration on "Strengthening independent and pluralistic information media" (especially in Central and Eastern Europe) September 13, 1997 and approved on 29-th session of the UNESCO General Conference (November 12, 1997), Okinawa Charter on global information society (from July 22, 2000) and the International Convention on Cybercrime (from November 13, 2002 adopted by the Committee of Ministers of the Council of Europe). Legal regulation is intended to facilitate development of the entire system of international cooperation in the field of informatization, in particular, the implementation of agreed international projects and programs.

It is obvious that the development of a global and secure information society is a complex process that requires constant monitoring, analysis and active international multilateral cooperation. Therefore, taking into account the progressive negative trends in international information environment, not only the positive dynamics of the international legal framework are necessary in the field of information security, but also further expansion of practical compromise inter-State interaction on various issues of cooperation in the field of ensuring international information security.

6. Conclusion

Information security is a complex system, multi-level phenomenon, the prospects of development of which are exposed to external and internal factors.

Components of information security are:

- The state of security of the information space, which is provided by its formation and development in the interests of citizens, organizations, States and the international community;
- The state of security of the information infrastructure, where information is used strictly for its intended purpose and will not have a negative impact on the system (object) when using it;
- The state of security of the information itself, which precluded or substantially hindered by violations of such properties as the confidentiality, integrity and availability.

Today, the basic legal principles of information security have been formulated, which should ensure:

- The integrity of the data-protection against failures, leading to loss of information, as well as unauthorized, unauthorized, illegal construction or destruction of data;
- Confidentiality (legitimacy) of the information;
- The availability of information for all authorized registered users;
- Protection of computer information from unlawful encroachment (copying, theft, distribution, forgery).

The main objectives of information security are:

- Protection of State information resources, as well as human rights and public interest in the information sphere;
- Preventing information dependence of the State, informational expansion or blockade by other States, informational isolation of senior officials and other State bodies and organizations.

The main tasks of information security of the countries are:

- Improvement of national legislation in the field of information security;
- Development of state information security policy, a set of measures and methods of its implementation;

- Coordinating the activities of State bodies and organizations in the field of information security;

- Development of the system of information security, improving its organization, forms, methods and means of neutralization of threats to information security, the elimination of the consequences of its violation.

Sources of threats to information security of the countries are:

- Individual foreign political, economic, military and information structures;
- Intelligence and special services of foreign countries;
- International terrorist and extremist organizations;
- Illegal political, religious and economic structures of the destructive direction;
- Organized criminal community and groups;
- Private individuals and legal entities;
- Natural disasters and catastrophes.

All in all information security can be defined as a specific condition of society, which provides comprehensive protection of the individual, society, the State and the international community in the real and virtual information space from exposure to specific threats, acting in the form of organized or spontaneously emerging internal and external information and communication flows.

References

[1] Meshkova T.A. Security in the context of global informatization: new challenges and new opportunities: Dissertation thesis…. Political Sciences, -M.: Moscow State University named after M.V. Lomonosov, 2003. – P. 4-5.

[2] Bashly P.N. Information security. -Rostov o/D : Phoenix, 2006. – P. 7-8.

[3] Bashly P.N. Information security. -Rostov o/D: Phoenix, 2006. – P. 7-8.

[4] Report of the UN General Assembly A/55/40, July 10, 2000; A/55/140/Add. 1, October 3, 2000; A/55/140/Corr. 1, October 3, 2000//Information calls for national and international security/edited by Fedorova A.V, Tsygichko V.N.- M:.PIR-Centre, 2011, - P. 315.

[5] http://www.un.org/ru/documents/ods.asp?m=A/C.1/53/3 - the official website of the UN (date of access)

[6] http://www.un.org/ru/documents/ods.asp?m=A/RES/53/70-the official website of the UN (date of access 05.02.2016)

[7] http://www.un.org/ru/documents/ods.asp?m=A/RES/54/49-the official website of the UN (date of access 05.02.2016)

[8] http://www.un.org/ru/documents/ods.asp?m=A/56/164/Add.I-the official website of the UN (date of access 05.02.2016)

[9] http://www.un.org/ru/documents/ods.asp?m=A/RES/56/19-the official website of the UN (date of access 12.03.2016)

[10] http://www.un.org/ru/documents/ods.asp?m=A/RES/62/17- the official website of the UN (date of access 03.03.2016)

[11] http://www.un.org/ru/documents/ods.asp?m=A/RES/66/24- the official website of the UN (date of access 23.03.2016)

[12] http://www.un.org/ru/documents/ods.asp?m=A/RES/68/243 the official website of the UN (date of access 03.05.2016)

[13] http://www.un.org/ru/documents/ods.asp?m=A/RES/69/28- the official website of the UN (date of access 12.05.2016)

[14] http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174&Lang=R– official website of the UN (report13 from Session 70of the UN General Assembly , July 22, 2015, A/70/174) (date of access 23.05.2016)

[15] http://www.un.org/ru/documents/ods.asp?m=A/RES/70/237-the official website of the UN (date of access 24.05.2016)

[16] http://www.un.org/ga/search/view_doc.asp?symbol=A/69/723&Lang=R - the official website of the UN Letter from the permanent representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations from January 9, 2015, addressed to the UN Secretary-General. Developments in the field of informatization and telecommunications in the context of international security. A/69/723. (Date of access 30.05.2016)

[17] Information and Communication Technologies I Development: A UNESCO Perspective: prepared by the UNESCO Secretariat. – Paris: UNESCO, 1996. - P.4.

[18] Committee on National Security Systems: National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, 26 April 2010.

[19] Venter, H. S., & Eloff, J. H. P. (2003). "A taxonomy for information security technologies". Computers & Security, 22(4). - P. 299–307.

[20] Anderson, J. M. (2003). "Why we need a new definition of information security". Computers & Security, 22(4). - P. 308–313.

[21] Lopatin V.N. "Information security in Russia: People. Society. State. "-St. Petersburg:" University" Fund, 2000. - P. 79.

[22] Szafransi R. A theory of Information Warfare. Preparing for 2020//Airpower Journal. -2005. -Spring. - P. 26.

[23] See: Libicki M. Conquest in cyberspace. National security and information warfare. -Cambridge, 2007. -P. 38.

[24] Manoylo A.V., Petrenko A.I., Frolov D.B. State information policy in terms of information and psychological warfare. M.: RAGS, 2007. –P. 524.

[25] http://cis.minsk.by/reestr/ru/index.html#reestr/view/text?doc=4074-the official site of the CIS (date of access 23.06.2016)

[26] https://ccdcoe.org/sites/default/files/documents/SCO-090616 - IISAgreementRussian.pdf- the official site of SCO (date of access 23.06.2016)

[27] Nugmanov N.A. International legal aspects of the regulation of legal relations in the field of information. Journal "International relations", UWED, Tashkent. - 2014. No. 3. - P. 79.

[28] http://www.un.org/ru/documents/ods.asp?m=A/RES/58/199-the official website of the UN (date of access 30.06.2016)

Author Profile

Nugmanov Nugman had Ph.D. degree in International Law from University World Economy and Diplomacy. He worked as an associate professor at the University of World Economy and Diplomacy, in "UNESCO`s International Law and Human Rights" Departmen. Since 2014 Vice-rector for scientific work of University of World Economy and Diplomacy